Article

Chinese Science Bulletin

Quantum Information

October 2013 Vol.58 No.28-29: 3514–3518
doi: 10.1007/s11434-013-6020-y

An efficient quantum meet-in-the-middle attack against NTRU-2005

WANG Hong, MA Zhi* & MA ChuanGui

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China

Received January 12, 2013; accepted May 15, 2013

NTRU is one of the most widely used public-key cryptosystems and its security has been an active research topic. This paper proposes a new way to find NTRU-2005 private key. The algorithm is based on meet-in-the-middle attack and a quantum algorithm for searching the fixed weight target. Compared with the current classical and quantum meet-in-the-middle attacks, our algorithm has lower time and space complexity. Moreover, this attack can also be applied against different versions of NTRU. The result can help to understand the security of NTRU better.

quantum algorithm, NTRU, meet-in-the-middle attack

Citation: Wang H, Ma Z, Ma C G. An efficient quantum meet-in-the-middle attack against NTRU-2005. Chin Sci Bull, 2013, 58: 3514–3518, doi: 10.1007/s11434-013-6020-y

For all the time, how to use the quantum computational theory to improve the classical cryptanalysis ability is an important issue. NTRU is a public-key cryptosystem based on the shortest lattice vector problem. At equivalent security level, NTRU needs lower memory and smaller computational complexity than RSA. Now, there is no efficient quantum algorithm known that will solve the shortest lattice vector problem. So, it is believed that NTRU is secure in quantum times [1]. In fact, with the rapid development of quantum computation, all cryptosystems based on the problems of large integer factorization and discrete logarithm are potentially fragile. However, it is still unclear what kind of effects the quantum computational theory could make on the security of NTRU till now.

Classical meet-in-the-middle (MITM) attack is a generic cryptanalytic method originally developed from cryptanalysis of block ciphers. Recently, this technique is also found to be quite useful in the cryptanalysis of public-key cryptography. MITM attack is the best algorithm for attacking NTRU at present. Grover [2] proposed a generic quantum search algorithm which gives a quadratic speedup over the classical brute-force search. However, it is not yet known whether Grover algorithm can speed up the classical MITM attack.

There are some new developments in the classical cryptanalysis of NTRU, such as lattice attack, hybrid attack [3], broadcast attack [4], etc. Ludwig [5] combined lattice reduction technique with Grover algorithm, and put forward a novel quantum attack algorithm against NTRU. However, the attack algorithm in [5] is not better than classical MITM attack. In 2011, a quantum algorithm used to find fixed weight target was proposed [6]. At the same time, the author analyzed the security of NTRU by the proposed algorithm. The computation complexity of Wang's algorithm is significantly lower than a classical brute-force search, but still higher than a classical MITM attack.

Xiong et al. [7] combined MITM attack with Grover quantum searching algorithm, and developed a quantum MITM attack method against NTRU. The time complexity in [7] is $O\left(\sqrt{C_{N/2+1}^{d/2}}\right)$, which is lower than the classical MITM attack $O\left(C_{N/2}^{d/2}/\sqrt{N}\right)$. However, the author just considered the quantum iterative times, and ignored all the complexity of classical precomputation. If considering the classical complexity, the complexity of MITM attack in [7]

*Corresponding author (email: ma_zhi@163.com)

is $O\left(C_{N/2+1}^{d/2}\log C_{N/2+1}^{d/2}\right)$, which has no any advantages compared with the classical MITM attack in [8].

Based on the classical MITM attack and a quantum algorithm to find a target solution with fixed weight, we propose a new quantum algorithm to attack NTRU. The time complexity is only $O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$ (Here, $\lfloor x\rfloor$ denotes the largest integer less than x), which is lower than previous attacks.

1 Preliminaries

1.1 NTRU cryptosystem

NTRU has been accepted as one of the standard public-key cryptosystem in the standard IEEE Std 1363.1. The advantage of NTRU over other cryptosystems is that encryption and decryption are very fast and the key are relatively small. Also the key generation is fast and easy. There have been several different versions of NTRU [9,10].

For the completeness, we give a simple description of NTRU key generation. Details can be found in [10]. To keep consistent with [6,7], we use the same notation (The versions in [6] is NTRU-2005).

In NTRU, given three integers N, p, q>0, and the basic objects are truncated polynomials in the ring $R=\mathbb{Z}_q[x]/\left(x^N-1\right)$. Every element in the ring R can be represented as a vector or a polynomial, where multiplication is defined as convolution multiplication.

There are three nonempty proper subsets:

$S_r,S_g,S_F\subseteq R$, where element $r\in S_r=S(d_1)$ means that there are d_1 coefficients of one in polynomial r, and the rest are zero; Similarly, one can define S_g=$S(d_2)$, S_F=$S(d_3)$.

Step 1 Randomly choose $g\in S_g$ and $F\in S_F$, calculate f=1+pF. Here we require that there exists $f_q\in R$ such that $f\times f_q\equiv 1(\text{Mod } q)$.

Step 2 Let $h=f_q g\ (\text{Mod } q)$.

The public key of NTRU: h, p, q.

The private key of NTRU: f.

1.2 A classical MITM attack

Choose an integer k, such that 2^k is much larger than $C_{N/2}^{d/2}$.

In [8], the private key f=F, and the public key h=$f_q g$ (Mod q);

Let f=$f_1\|f_2$, where both f_1 and f_2 have a length of N/2, containing d/2 ones, and $\|$ denote concatenation.

(1) Enumerate f_1. Put each f_1 into a "bin" based on the most significant bits of the first k coordinates of f_1h(Mod q);

(2) Enumerate f_2. Judge each f_2 to see if it corresponds to an occupied bin. While checking for occupation, we consider not only the bin given by the most significant bits of the first k coefficients of $-f_2h$(Mod q), but also the bins given by the flips of all the most significant bits which add 1 to the corresponding coefficients of $-f_2h$(Mod q);

(3) Search for matches. When f_2 hits an occupied bin, take f_1 from the bin. Determine whether $(f_1\|f_2)\times h$(Mod q) is binary, and if so return f=$f_1\|f_2$ and terminate. Otherwise, proceed to the next f_2. Check each one if the bin contains more than one f_1.

The algorithm can always return the private key f or a cyclic shift of f. Both the time and space complexity are $O(C_{N/2}^{d/2}/\sqrt{N})$.

1.3 Wang's attack algorithm

Wang et al. [6] put forward a quantum algorithm to find the fixed weight target, and proposed a new method to find the private key of NTRU. Wang's algorithm can be considered as a quantum brute-force attack, which can reduce the time complexity from $O\left(C_N^d\right)$ to $O\left(\sqrt{C_{N+1}^d}\right)$.

First, Wang et al. define the label of an n-dimensional Boolean vector with fixed weight.

Definition 1 [6] Suppose that the weight of an n-dimensional Boolean vector v is w, that is, in all positions v takes value 0 except at positions a_1, a_2,...,a_w with 1⩽a_1<a_2<...a_w⩽n.

The label L_v of vector v is then defined as

$$L_v=1+C_{a_1}^1+C_{a_2}^2+...+C_{a_w}^w.$$

Obviously, there is a one-to-one correspondence between vectors and their labels.

Moreover, $C_{w+1}^w\leqslant L_v\leqslant C_{n+1}^w$. The label of a target vector is called the target label.

Wang's attack procedure is as follows:

(1) Compute the maximum value of labels C_{n+1}^w, denote $t=\lceil\log C_{n+1}^w\rceil$;

(2) Search the t-tuple vector using Grover algorithm, derive the target label;

(3) Derive target vector from target label, return as a candidate private key.

1.4 A quantum MITM Attack

In [7], the author assumed N and d are even; The bin which contains polynomial f_i will be labeled as label_f_i, and $\text{bin}(f_i)=\{\text{label}\_f_i\}$.

The basic idea of quantum MITM attack in [7] is:

(1) Compute all $\{\text{label}\_f_1,f_1\}$ and arrange as a table L indexed by label_f_1;

(2) Search f_2 with the Grover search algorithm, with $\text{label}\_f_1\in\text{bin}(f_2)$, and

$$(f_1 + f_2)h \,(\text{Mod } q) \in \{0,1\}^N;$$

(3) Search f_1 correspond to label$_f_1$ in L; Verify f_1+f_2 with other conditions.

In fact, the time complexity analysis in [7] is incorrect. Just as we mentioned before, the author ignored all the complexity of classical precomputation.

2 An improved quantum MITM attack

In NTRU-2005, the private key is f=1+2F, where polynomial (or vector) F is consisting of d ones and N–d zeros.

So, if we can find the polynomial F, the private key f can also been obtained easily. Here, the polynomial F can also be regarded as a vector.

The basic idea of the improved algorithm

The idea is to find the key F in the form $F_1 \| F_2$, where $\|$ denotes concatenation. The length of F_1 and F_2 are $\lfloor N/3 \rfloor$ and $N-\lfloor N/3 \rfloor$, respectively. Moreover, F_1 has $\lfloor d/3 \rfloor$ ones, and F_2 has $d-\lfloor d/3 \rfloor$ ones.

We have

$$fh = g \,(\text{Mod } q)$$
$$\Rightarrow \left[1+2\left(F_1 \| F_2\right)\right]h = g \,(\text{Mod } q)$$
$$\Rightarrow h + F_1 \times 2h = g - F_2 \times 2h \,(\text{Mod } q)$$
$$\Rightarrow h_i + \left(F_1 \times 2h\right)_i = \{0,1\} - \left(F_2 \times 2h\right)_i \,(\text{Mod } q) \forall i$$

In fact, according to lemma 1, although F itself may not have the property, we know that there exist some rotations of F which has this property and that any rotation of F will be effective as the private key parameters.

Lemma 1 Let $F = F_1 \| F_2$, $\lfloor N/3 \rfloor$ and $N-\lfloor N/3 \rfloor$ are the length of F_1 and F_2, respectively. Then there exists one rotation of F which has the property: F_1 has $\lfloor d/3 \rfloor$ ones, and F_2 has $d-\lfloor d/3 \rfloor$ ones.

Proof Let a, b>0. Without loss of generality, let F has $\lfloor d/3 \rfloor + a$ ones in the first $\lfloor N/3 \rfloor$ entries, b ones in the middle $\lfloor N/3 \rfloor$ entries, and $d-\left(\lfloor d/3 \rfloor + a\right)-b$ ones in the last $N-2\lfloor N/3 \rfloor$ entries.

Then, rotating F by one position can only change the number of ones in the first (middle) $\lfloor N/3 \rfloor$ entries by 0, 1 or –1. There are three cases:

In case 1, if $b = \lfloor d/3 \rfloor$, then after $\lfloor N/3 \rfloor$ left rotations each at a position, obviously;

In case 2, if $b < \lfloor d/3 \rfloor$, when finishing $\lfloor N/3 \rfloor$ left rotations, the first $\lfloor N/3 \rfloor$ entries will have $b < \lfloor d/3 \rfloor$ ones in them. Therefore, at some points, the number of ones in the first $\lfloor N/3 \rfloor$ entries must have been exactly $\lfloor d/3 \rfloor$;

Now let us look at the last case. If $b > \lfloor d/3 \rfloor$, then $d-\left(\lfloor d/3 \rfloor + a\right)-b < \lfloor d/3 \rfloor$, so after $N-\lfloor N/3 \rfloor$ left rotations, the first $N-2\lfloor N/3 \rfloor$ entries will have

$$d-\left(\lfloor d/3 \rfloor + a\right)-b < \lfloor d/3 \rfloor$$

ones in them, obviously.

Let T and S denote the binary vectors which are defined by the most significant bits of the first k coordinates of $h + F_1 \times 2h \,(\text{Mod } q)$ and $-F_2 \times 2h \,(\text{Mod } q)$, respectively. Here, all F_1 are of length $\lfloor N/3 \rfloor$, but we identify them with the length-N vectors formed by appending $N-\lfloor N/3 \rfloor$ zeros. Similarly, we identify all F_2 with the length-N vectors formed by prepending $\lfloor N/3 \rfloor$ zeros.

Algorithm 1

(i) Choose an integer k, so that

$$2^k \geqslant 100 * C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor};$$

(ii) Calculate each F_1 to get the binary vector T, and arrange as a table L indexed by T;

(iii) Apply the Oracle, let F_2 run over its whole sample space and then, search for matches by quantum algorithm in [6]. The proper matches meet the two conditions:

(1) $S \in \{T\}$ or $S' \in \{T\}$, where S' is given by the flips of some bits of S which add 1 to the corresponding coefficients of $-F_2 \times 2h \,(\text{Mod } q)$;

(2) $h + \left(F_1 \| F_2\right) \times 2h \,(\text{Mod } q) \in \{0,1\}^N$;

(iv) Verify $f = 1 + 2\left(F_1 \| F_2\right)$ with other conditions.

Details of searching for matches in step (iii) are:

(1) Let the label l correspond to the vector $F_{2,l}$. The Oracle can be defined as

$$O(l) = \begin{cases} 1, \text{if } F_{2,l} \text{ meet the two conditions in step (iii);} \\ 0, \text{others;} \end{cases}$$

(2) Calculate the maximum value of the label $C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor}$, let $n = \left\lceil \log C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor} \right\rceil$;

(3) Initialize the quantum system, and produce the equally-weighted superposition state $\frac{1}{2^{n/2}} \sum_{l=0}^{2^n-1} |l\rangle |0\rangle$;

(4) Use Grover algorithm $\pi 2^{n/2}/4$ times, get the label l and the vector $F_{2,l}$ correspond to the label.

Algorithm analysis

Let $O(\cdot)$ denote the complexity of classical computation; Similarly, $\bar{O}(\cdot)$ denotes the complexity of quantum computation. Furthermore, to keep consistent with [1,8], the time to calculate $h + F_1 \times 2h \,(\text{Mod } q)$ is taken to be one

Table 1 Time and space complexity comparison for different NTRU attacks

	C-MITM [8]	Wang's attack [6]	Q-MITM [7]	This paper
Time	$O\left(\frac{C_{N/2}^{d/2}}{\sqrt{N}}\right)$	$O\left(\sqrt{C_{N+1}^{d}}\right)$	$O\left(C_{N/2}^{d/2}\log C_{N/2}^{d/2}\right)$ $+\bar{O}\left(\sqrt{C_{N/2+1}^{d/2}}\right)$	$O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$ $+\bar{O}\left(\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}}\right)$
Space	$O\left(\frac{C_{N/2}^{d/2}}{\sqrt{N}}\right)$	$O(1)$	$O\left(C_{N/2}^{d/2}\right)$	$O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$

Table 2 Time complexity comparison for various parameters

	C-MITM [8]	Wang's attack [6]	Q-MITM [7]	This paper
Time complexity	$O\left(\frac{C_{N/2}^{d/2}}{\sqrt{N}}\right)$	$O\left(\sqrt{C_{N+1}^{d}}\right)$	$O\left(C_{N/2}^{d/2}\log C_{N/2}^{d/2}\right)$ $+\bar{O}\left(\sqrt{C_{N/2+1}^{d/2}}\right)$	$O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$ $+\bar{O}\left(\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}}\right)$
NTRU251	2^{80}	$2^{86.5}$	$2^{91.3}+2^{42.6}$	$2^{61.3}+2^{57.3}$
NTRU347	2^{112}	$2^{119.8}$	$2^{124.9}+2^{59.2}$	$2^{83.9}+2^{79.5}$
NTRU491	2^{160}	$2^{167.7}$	$2^{173.3}+2^{83}$	$2^{115.4}+2^{111.7}$
NTRU587	2^{192}	2^{200}	$2^{205.7}+2^{99.2}$	$2^{137.8}+2^{132.9}$

operation.

According to the above process, the time and space complexity of algorithm 1 depend on step (ii) and step (iii).

The number of F_1 is $C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}$, so the time to put each F_1 into a proper bin is $O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$;

Calculating the table L needs $O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$ basic operation. So the expected time to run step (ii) will be no more than $O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$;

The computation complexity of step (iii) only depends on Grover iterative times, i.e. $\bar{O}\left(\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}}\right)$;

The table L needs to be saved, so the space complexity is $O\left(C_{\lfloor N/3+1\rfloor}^{\lfloor d/3\rfloor}\right)$.

3 Comparison for different NTRU attacks

The comparisons of results for different attacks and various parameters are illustrated in Table 1 and Table 2.

Remark Compare the two tables above, our method is very efficient both in the time and space complexity.

In fact, if quantum computation is not more expensive than classical computation, it would be worthwhile to transfer some ones from the F_1 side to the F_2 side. In this case, the expected running time become approximately

$$O\left(\sqrt{\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}}\cdot C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}}\cdot\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right).$$

4 Conclusions

With the development of quantum computation, the security strength of NTRU has been an active research area in the past 10 years. This paper revised some errors in [7] and proposed an improved quantum MITM attack against NTRU. The time complexity in this paper is significantly reduced. Moreover, this attack can also be applied against NTRU-1998 and NTRU-2001. The result can help to understand the security of NTRU better. An open question worth investing would be to see if the current attacks may still be improved.

This work was supported by the National High Technology Research and Development Program of China (2011AA010803), the National Natural Science Foundation of China (U1204602) and the Open Project Program of the State Key Laboratory of Mathematical Engineering and Advanced Computing (2013A14).

1 Perlner R A, Cooper D A. Quantum resistant public key cryptography: A survey. In: Seamons K, McBurnett N, Polk T, eds. Proceedings of the 8th Symposium on Identity and Trust on the Internet, 2009 April 14–16, Gaithersburg, MD, USA. New York: ACM Press, 2009. 85–93

2 Grover L K. A fast quantum mechanics algorithm for database search. In: Proceeding of the 28th ACM Symposium on Theory of Computation, Philadelphia, PA, USA. New York: ACM Press, 1996. 212–219

3 Howgrave-Graham N. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: Menezes A, ed. Proceedings CRYPTO, 2007 August 19–23, Santa Barbara, CA, USA. Berlin Heidelberg: Springer, LNCS 4622, 2007. 150–169

4 Ding J T, Pan Y B, Deng Y P. An algebraic broadcast attack against NTRU. In: Susilo W, Mu Y, Seberry J, eds. Proceedings ACISP, 2012 July 9–11, Wollongong, NSW, Australia. Berlin Heidelberg: Springer, LNCS 7372, 2012. 124–137

5 Ludwig C. A faster lattice reduction method using quantum search. In: Ibaraki T, Katoh N, Ono H, eds. Proceedings ISAAC, 2003 December 15–17, Kyoto, Japan. Berlin Heidelberg: Springer, LNCS 2906, 2003. 199–208
6 Wang X, Bao W S, Fu X Q. A quantum algorithm for searching a target solution of fixed weight. Chin Sci Bull, 2011, 56: 484–488
7 Xiong Z, Wang J, Wang Y, et al. An improved MITM attack against NTRU. Int J Sec App, 2012, 6: 269–274
8 Silverman J, Odlyzko A. NTRU Report 004, Version 2, A Meet-The Middle Attack on an NTRU Private Key. Technical Report, NTRU Cryptosystems, 2004
9 Hoffstein J, Pipher J, Silverman J. NTRU: A ring-based public key cryptosystem. In: Buhler J P, ed. Proceedings Algorithmic Number Theory (ANTS III), 1998 June 21–25, Portland, Oregon, USA. Berlin Heidelberg: Springer, LNCS 1423, 1998. 267–288
10 Howgrave-Graham N, Silverman J H, Whyte W. Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In: Menezes A, ed. Proceedings the Cryptographers' Track at the RSA, 2005 February 14–18, San Francisco, CA, USA. Berlin Heidelberg: Springer, LNCS 3376, 2005. 118–135